ISE SHARED SPACES AND CORE: DISCUSSION PAPER FOR THE ISC

JULY 2, 2008

TABLE OF CONTENTS

1 Document Purpose and Intended Audience

This paper responds to a tasking from members of the Information Sharing Council[1] (ISC) to address the question "What is an Information Sharing Environment (ISE) Shared Space?" In developing the paper, we realize that "What is an ISE Core?" is also a relevant and appropriate question to address at this time. To address both questions completely and formally, this paper first provides in Section 2 the context for ISE Shared Spaces and ISE Core, as developed in the ISE Enterprise Architecture Framework.[2] Then, Section 3 provides both general and technical definitions of ISE Shared Space and ISE Core. Going beyond definitions, Section 4.1 presents three implementation models for ISE Shared Spaces. Section 4.2 provides implementation models for ISE Core as both common services and infrastructure. Taken all together, the sections in this paper provide overarching descriptive concepts and approaches that may be used by ISE participants in identifying existing infrastructure to implement the ISE (either a Shared Space or Core) or in planning for and establishing an ISE Shared Space or Core. Section 5 presents a summary and suggestions for further discussion.

While this paper is in response to a question from members of the Information Sharing Council (ISC), the intended audience also includes program managers and systems/network designers of information technology resources in ISE participant organizations that will be responsible for leveraging existing infrastructure, planning, designing, and installing their organization's ISE Shared Spaces or Core.

2 Context[3]

As envisioned for today, the ISE infrastructure comprises two key components: (1) ISE Shared Spaces and the (2) ISE Core.[4] These two components derive from a statement of need, a set of mandates, and a number of foundational concepts and assumptions.

2.1 Statement of Need

The long-term vision for information sharing within the ISE is to allow authorized users (investigators, analysts, others with various missions) to search, discover, and access data when needed. Search and discovery involves conducting queries of disparate information and finding

[1] Executive Order 13356 established a Council to review matters related to the improvement of sharing terrorism information. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) changed the name of this Council to the Information Sharing Council and provided it responsibilities to advise the President and the Program Manager on the development of ISE policies, procedures, guidelines, and standards, and to ensure proper coordination among federal agencies participating in the ISE. Under the Obama Administration, the ISC has been integrated into the White House policy process through the Information Sharing and Access Interagency Policy Committee (IPC), so that the important work of the ISC will move forward under the auspices of the Executive Office of the President.

[2] ISE Enterprise Architecture Framework, version 1.0, August 2007, available at http://www.ise.gov/docs/eaf/ISE-EAF_v1.0_20070830.pdf.

[3] This section highlights the references and key concepts that led to the formation of the ISE Share Space vision and definition. Much has been written about the ISE in general and interested readers are referred to http://www.ise.gov/pages/vision.html.

[4] ISE Enterprise Architecture Framework, version 1.0, August 2007, available at http://www.ise.gov/docs/eaf/ISE-EAF_v1.0_20070830.pdf.

data from sources a user may otherwise not know exist. Users will be allowed access to structured, unstructured, finished, unfinished, and source information as appropriate, depending on their mission needs, clearances, and other access privileges.[5] Achieving this vision requires development and/or implementation of several expanded features of highest priority:

- First, systems must be compatible and have the capability to interconnect. Information can only be searched, discovered, and accessed if the user has the necessary cyber connectivity.
- Second, there must be a robust access and identity management capability, allowing users to access only that data for which they are authorized. Organizations will not make their information available to others unless adequate protection is provided. Without access and identity management services to provide that protection, organizations will block access to their data.
- Third, systems must provide proper levels of protection for information that moves between users or organizations at each security level.
- Fourth, because of the management difficulties associated with multiple accounts and passwords, long-term technical capabilities should support single sign-on for users.[6]
- Fifth, there must be an agreed standard for user vetting and account provisioning and de-provisioning. Today's schemes vary by organization.
- Finally, there must be agreement on system certification and accreditation standards; multiple standards are currently in use.

These dependencies are representative components of what is commonly referred to as *system trust*. Without system trust, organizations are reluctant to share their information because of the risk that information could be lost, corrupted, or otherwise compromised.

The long-term ISE vision requires organizations to develop and accept a level of system trust much higher that that which exists today. Growing that trust depends on policy and cultural changes that support authorized access for all ISE participants. While ISE partners currently share information and have made significant progress since 9/11, further enhancement opportunities are envisioned. Sharing mechanisms today include, but are not limited to, the ability for a user to access information that another organization has made available in a protected access repository; the use of subscription services to direct selected data to authorized consumers; posting of information on Web pages; and relay of information by e-mail. Such sharing techniques remain valuable and will continue to be used for sharing information pending implementation of the envisioned end-state.

For the intervening period, there is a continued need to enhance the amount and timeliness of information being shared. After considering a number of potential approaches, the concept of ISE Share Spaces and ISE Core has been developed for information sharing today.

[5] The long-term vision of the ISE includes the sharing, as appropriate, of various forms of source, or raw, data. If a user has access only to finished products and the authors of those products have failed to "connect the dots" then the user will not have the info needed to connect the dots either.

[6] This requires a community-accepted ID management approach.

2.2 Mandates

The Intelligence Reform and Terrorism Prevention Act, as amended (IRTPA), requires the ISE to facilitate the sharing of terrorism, homeland security, and weapons of mass destruction information[7] within and among all levels of governments and the private sector, and at all levels of security classifications.

To accomplish this sharing, the concept of ISE Shared Spaces has been developed to address immediate shortfalls and is documented within the ISE Enterprise Architecture Framework (ISE EAF). The ISE Shared Spaces are where information is shared based upon clearly identified ISE-level mission need for such information and commonly agreed to business processes and information flows. The ISE Core is the infrastructure made up of enterprise services, networks and systems that interconnect the individual ISE Shared Spaces into a functioning unified network.

Many specific examples demonstrate that sharing today is occurring using the ISE Shared Spaces and ISE Core approach. The Terrorist Identities Datamart Environment (TIDE), hosted by the National Counter-Terrorism Center (NCTC) and distributed by the Terrorist Screening Center (TSC) is one example. Also, law enforcement information shared by Department of Justice (DOJ) through OneDOJ and Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE) through Regional Sharing System are both standardized shared spaces. However, both of these examples can be improved to ensure the information is accessible by all appropriate ISE participants.

Recognizing the breadth of participants the ISE is intended to unify, ISE Shared Spaces and ISE Core also provide the means for ISE participants with national security system (NSS)[8] network assets, historically sequestered with only other NSS systems, to interface with ISE participants having only civil network assets. Furthermore, ISE Shared Spaces and ISE Core also provide the means for foreign partners to interface and share terrorism information with their U.S. counterparts.

In short, ISE Shared Spaces and ISE Core allow ISE participants to leverage, for information sharing purposes, their technologies and processes that are tightly coupled to their missions to support the larger national counterterrorism (CT) mission called for by the President in National Strategy for Information Sharing (NSIS), the Congress in IRTPA, and the 9/11 Commission.

---

[7] As recommended in the ISE Implementation Plan, the ISE has also been expanded to include the sharing of law enforcement information related to terrorism. Formal definitions of ISE-related information are available at http://www.ise.gov/pages/scope.html.

[8] 40 U.S.C. Section 11103(a) defines a *national security system* as "a telecommunications or information system operated by the Federal government, the function, operation, or use of which: (A) involves intelligence activities; (B) involves cryptologic activities related to national security; (C) involves command and control of military forces; (D) involves equipment that is an integral part of a weapon or weapons system; or (E) subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions. (2) Limitation.-Paragraph (1) (E) does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personal management applications)."

2.3 Foundational Concepts and Examples

Establishing and applying standards to information is a commonly-used mechanism to enhance organizational ability to share that information. The standards for ISE Shared Spaces and ISE Core are documented by the Common Terrorism Information Sharing Standards Program (CTISS).[9] Consistent with the discussion above, CTISS are formally defined as business process-driven, performance-based common standards for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. From a data standards standpoint, CTISS can apply to both structured and unstructured information.

As stated in the ISE Implementation Plan, "terrorism information sharing and interoperability with the ISE need to be integral attributes of departments' and agencies' overall information resource planning and enterprise architectures."[10] As such, both ISE Shared Spaces and ISE Core include a capital planning and investment perspective consistent with requirements specified through the White House Office of Management and Budget (OMB) regarding the Capital Planning and Investment Control (CPIC) and Federal Enterprise Architecture (FEA) programs.

A key challenge in this work is identifying, organizing, and prioritizing the information sharing needs of the national CT mission. Using the framework of the Intelligence Cycle,[11] information sharing needs can be grouped into two categories: (1) supporting, enabling, and improving dissemination activities with structured, vetted, and finished information products and (2) supporting, enabling, and improving the sharing of information used and needed throughout the cycle. The general belief is that improvements in category 1 are easier to achieve than in category 2. Fortunately, ISE Shared Spaces and ISE Core can support, enable, and improve sharing in both categories.

3 Definitions

3.1 General

ISE Shared Space: An ISE Shared Space is where standardized terrorism information, as defined through the Common Terrorism Information Sharing Standards (CTISS), is made available by one ISE participant to others, as appropriate. Additionally, ISE participants may create or use an ISE Shared Space to make services accessible, as appropriate, to other ISE participants.

ISE Core: The ISE Core provides infrastructure and services necessary for the interconnection and use of information made available through ISE Shared Spaces. ISE Core exists within and across three information security domains (i.e., TS/SCI, Secret/Collateral, and Sensitive but Unclassified (SBU)).

[9] As defined in ISE Administrative Memorandum-300, available at http://www.ise.gov/docs/ctiss/ise-asm300-ctiss-issuance.pdf

[10] PM-ISE, *ISE Implementation Plan* (Washington: PM-ISE, 2006), page 107.

[11] For discussion here, the Intelligence Cycle has 5 activities: planning and direction, collection, processing, analysis and production, and dissemination. This cycle is used for example only, other information or knowledge management cycles, like law enforcement investigation cycle or the O-O-D-A Loop, are equally relevant.

3.2 Technical

ISE Shared Space: ISE Shared Space consists of hardware and software that serve as the participant's infrastructure for ISE activity, as defined through the Common Terrorism Information Sharing Standards (CTISS). There may be multiple ISE Shared Spaces, each under the management, control, and resourcing responsibility of the ISE participant. This responsibility includes ensuring information security, data integrity, use, retention, and other data stewardship requirements are met and that the ISE Shared Space capability supports established ISE mission processes.

ISE Core: The ISE Core has three major components: core services, portal services, and core transport. ISE Core Services provides ISE-level services used in operating the ISE (e.g., Access and Identity Management, Discovery and Search, Manipulation and Storage, Dissemination, Electronic Directory Services, Collaboration, Information Protection). ISE Core Portal Services provide the infrastructure for those services used in interfacing ISE portals to the Core (including Network Management). ISE Core Transport entails the underlying telecommunications infrastructure (e.g., cables, routers, switches) which moves ISE data and information from one ISE Shared Space to another.

4 Models

4.1 ISE Shared Spaces

In describing ISE Shared Spaces for identifying existing infrastructure to implement an ISE Shared Space or in planning for and establishing an ISE Shared Space, three models are to be considered:

- Establishing an information flow-driven model for an ISE Shared Space,
- Logical view model (or system-independent operational descriptions), and
- Hosting and implementation model.

These models support ISE participants in their development of enterprise, segment, and solution architectures[12] that clearly identify the structure and attributes of the organization's ISE Shared Spaces in sufficient detail to support fiscal year programmatic plans for information technology business case justification, acquisition, installation, operations, and management.

4.1.1 Information Flow Model

The information flow model for implementing an ISE Shared Space considers the mission or business drivers for organizations to follow in interfacing with the ISE. This model takes into

[12] Segment architecture refers to a business-driven approach to defining and designing, in addition to other supporting architectural components, each ISE participant's ISE Shared Space. It leverages the Federal Enterprise Architecture Consolidated Reference Model (CRM), the ISE EAF, and the Federal Transition Framework Catalog to build a layered architecture. Solution architecture refers to a business-driven approach to develop shareable assets and information technology components in support of business processes identified in the ISE EAF and participant segment architectures.

account not only the requirements of ISE participants that produce ISE information but also the information needs of other ISE participants consuming another ISE participant's information. These essentials are easily identified from the defined information flows from mission business processes that define the ISE. These drivers include

- *Specific Mission*: These information flows would be based on defined ISE mission business processes presenting relationships, exchanges, and products for terrorism information sharing. Functional standards of the CTISS define the business processes, information flows, and structured data (data elements and schema) that make up terrorism information products within these information flows for storage in an ISE Shared Space. A current example of this is Suspicious Activity Reporting (SAR), which has a well-defined information flow and associated Functional Standard (ISE-FS-200) and defined data and information for sharing in an ISE Shared Space.
- *Community*: These information flows would be based on mission business processes of participating organizations that make up a community of interest (COI). They may be associated with defense, homeland security, intelligence, foreign affairs, or law enforcement representative organizations with business processes that are part of that select community. Outputs of these COI processes may be data and information structured under CTISS for storage in an ISE Shared Space.
- *Entity*: These information flows would be based on mission business processes of an individual organization (i.e., 'entity'). For example, they may be processes associated with the immigration mission business process which specifically aligns with DHS' Immigration and Customs Enforcement agency.

4.1.2 Logical Model

The logical model identifies three general implementation schemes:

- *Replication*: Storage of terrorism information from internal resources into an ISE Shared Space and making it accessible to other ISE participants using common services, such as discovery, search, and directory services for access and use. A common example of this scheme would be libraries that provide the general public on-line card catalog services for locating books yet also maintain their book records on their own internal systems for inventory and management purposes.
- *Web-Service*: Exposing terrorism information, services, and applications via Web services that interface with other ISE participant Web portals. A common example of this is the approach used by on-line shopping vendors to make product information and sales services accessible to the general public via the Internet.
- *Hybrid*: Allowing direct access, with appropriate access management safeguards, to selected applications within an ISE participant's infrastructure. For example, collaborative use of a Case Management application used by two or more agencies cooperating in a joint CT investigation. Access would be granted after validating and ensuring appropriate authenticating credentials have been verified. An example of this scheme is police departments' accessing DOJ's Joint Automated Booking Systems (JABS).

4.1.3 Hosting and Implementation Model

Given the logical information flow and models, various hosting and implementation options are available to establish a participant's ISE Shared Space. These hosting options include:

- *Department Level*: A department, agency, or other ISE participating organization would establish an ISE Shared Space or multiple Spaces to facilitate terrorism information sharing for the entire organization, to include assigned bureaus and subordinate offices. The ISE Shared Space(s) would be interconnected with other ISE participants to provide access to standard information. An example of such a department-wide application for providing a comprehensive repository of information is the FBI's *Regional Data Exchange (R-DEx)* or One-DOJ system. One-DOJ is designed to provide the capability to share full text law enforcement investigative information from Federal, State, and local investigative agencies working in association with the FBI. From an overarching programmatic perspective, in this option an ISE participant would continue to be responsible for the overall budgeting, resourcing, and installation of the ISE Shared Space on behalf of the entire organization and its affiliated offices.
- *Component/Other Level*: An organizational element or subcomponent of the larger department, agency, or ISE participant would be responsible for establishing an ISE Shared Space supporting that component's responsibilities for interfacing with the ISE. An ISE Shared Space, established by this component, would be a portion of the network infrastructure operated and maintained by this component and would provide an ISE interface on behalf of the entire organization. An example of such an implementation scheme is DHS's *Regional Sharing System (RSS)* that is under the responsibility of the Immigration and Customs Enforcement (ICE) agency providing bi-directional information sharing capabilities between the Federal Government and State and local partners.
- *Third Party Level*: ISE participants may leverage the services and infrastructure of another third party service provider, who is a member of the ISE community, for "virtually" establishing their ISE Shared Space. Such an implementation option should be consistent with overall concepts for an ISE Shared Space as outlined in the ISE EAF and this paper. ISE participants, leveraging a third party service provider to host their ISE Shared Space, should have well-defined service level agreements (SLAs) to address the issues of resourcing, management, continuity of operations, data stewardship, and ownership. If an ISE participant expects/intends to leverage a third party service provider, any and all implications for operations would not be the sole responsibility of the ISE third party service provider. For example, if Department X decides to permit another department or agency to host its data for sharing in an ISE Shared Space, Department X remains ultimately responsible for the data stored and consumed within the third party resources servicing Department X's ISE Shared Space.

4.2 ISE Core

Elements of the ISE Core are resourced, planned, installed, and operated by designated Implementation Agents. The Implementation Agent's proposed enterprise, segment, and solutions architectures will clearly identify the structure and attributes that implement the

ISE Core segment in sufficient detail to support the investment and allow other ISE participants to plan their ISE Shared Spaces appropriately.

A number of key assumptions are made with regard to ISE Core Implementation Agents:

- Configuration management and systems integration are best accommodated with a single, designated implementation agent (may also be called Service Provider) within each information security domain (i.e., TS/SCI, Secret/Collateral, and SBU). Robust configuration management processes must be in place in the event of multiple Implementation Agents.
- Security policies and practices, whether originating in one community or not, must be ubiquitous within each security domain of the ISE Core and between implementation agents.
- Service Level Agreements (SLAs) will provide the necessary Quality of Service requirements and parameters for servicing the ISE Core.

4.2.1 Hosting and Implementation Model

Various hosting and implementation options are available to establish a participant's ISE Core. These options include:

- *ISE Implementation Agent:* A designated primary implementation agent is responsible for resourcing and providing all or a portion of the ISE Core to ISE participants represented in the defense, homeland security, law enforcement, intelligence, and foreign affairs communities. Outsourcing of some services is an acceptable option; albeit SLAs will exist for all services, regardless of secondary outsourcing agents, to ensure Quality of Service is maintained across the ISE. Program management and operations oversight are the responsibility of the primary Implementation Agent.
- *Single Community Implementation Agent*: A designated primary implementation agent responsible for resourcing and providing all or a portion of the ISE Core to ISE participants in a particular community (i.e., defense, homeland security, law enforcement, intelligence, or foreign affairs). Outsourcing of some services is an acceptable option; albeit SLAs will exist for all services, regardless of secondary outsourcing agents, to ensure Quality of Service is maintained across the ISE. A joint SLA also exists between the other communities and each Single Community Implementation Agent. Program management and operations oversight over all Implementation Agents is conducted through a designated department, agency, or other governmental organization.
- *Community Partnering Implementation Agent:* Two or more communities or ISE participants join together to identify and resource a designated primary service provider for their respective communities or share service provider responsibility redundantly for enhanced performance (ex., Redundant Arrays of Inexpensive Disks). Outsourcing of some ISE Core services are an option; albeit SLAs exist exclusively between this designated Implementation Agent and other community ISE participants. A joint SLA exists between Implementation Agents with program management and operations oversight by a designated department, agency, or other governmental organization.

5 Summary and Additional Issues for Discussion

ISE Shared Space and ISE Core are key concepts in developing system trust within the ISE today. Both have general and technical definitions, and a variety of models must be considered when selecting existing systems or developing an ISE Shared Space or ISE Core that meets the agreed upon standards for improving mission-related information sharing.

Different combinations of the models may be followed by an ISE participant for implementation. In all cases, however, an ISE Shared Space and ISE Core must be based upon a clearly identified ISE-level mission need for such information and commonly agreed to business processes and information flows. Such a standardized approach resolves the information processing and usage problem by providing places where alignment of information sharing policies, business processes, technologies, and systems occurs.

The concepts here support discussions and planning efforts concerning difficult implementation issues critical to success, such as:

Concept	Applicable FEA ISE profile area
Connectivity	Component framework / Data management
Search and Discovery	Service interface & integration / interface
Access and Identity Management	Service access & delivery identity management
Information Security	Information & Technology Management / Information Security
Funding and resource management	Management of Government Resources / Financial & HR Management
Governance	Business Management Services / Management of Process